

# **EXHIBIT A**

(Eighth Witness Statement, D. Holden)

Filed on behalf of the Proposed Appellant  
Statement of Dominic Holden  
Exhibit DPH8  
Date: 24 August 2020

**IN THE COURT OF APPEAL  
OF ENGLAND AND WALES**

**Ref: A3/2020/1271**

**ON APPEAL FROM THE HIGH COURT OF JUSTICE  
BUSINESS AND PROPERTY COURTS OF  
ENGLAND AND WALES  
BUSINESS LIST (ChD)**

**Claim no. HC-2016-002798**

**B E T W E E N:**

**FARHAD AZIMA**

**Proposed Appellant /  
Defendant and Counterclaimant**

**-and-**

**RAS AL KHAIMAH INVESTMENT AUTHORITY**

**Proposed Respondent /  
Claimant and Defendant to Counterclaim**

---

**EIGHTH WITNESS STATEMENT OF DOMINIC HOLDEN**

---

I, Dominic Holden, Partner at Burlingtons Legal LLP ("**Burlingtons**"), of 5 Stratford Place, London W1C 1AX **SAY AS FOLLOWS:-**

**I. Introduction**

1. I am the same Dominic Holden who provided witness statements in these proceedings before the High Court. Since Burlingtons' instruction by the Defendant in late June 2019, I have had responsibility (with other fee earners working under my supervision) for the conduct of these proceedings on behalf of Mr. Farhad Azima, the Proposed Appellant (and Defendant and Counterclaimant). I am authorised by Mr. Azima to make this statement on his behalf.
2. Unless stated otherwise, the facts set out below are within my own knowledge or are derived from my instructions and the documents which I have seen which in all cases

I believe to be true. Where any facts are not within my knowledge, the source of those facts is stated.

3. There is now produced and shown to me a bundle of documents marked "Exhibit DPH8" to which reference will be made in the course of this statement in the form '[DPH8/[page number]]'.
4. Where in this statement I refer to the existence of legal advice, or to communications with third parties that were undertaken for the dominant purpose of these or other proceedings, this should not be regarded as a waiver of privilege.

## **II. Purpose of this witness statement**

5. I provide this witness statement for the following related purposes.
6. First, it is filed in support of Mr. Azima's application for permission to rely upon fresh evidence in support of his application for permission to appeal to the Court of Appeal from the Order of Deputy Judge Andrew Lenon QC made on 17 July 2020 (and in support of his appeal, should permission to appeal be granted). There are two categories of new evidence:
  - a. First, Mr Azima's advisers have recently received data from Mr Raphael Satter, an investigative journalist at a well-known international news agency based in New York, Thomson Reuters ('TR'), which indicate that more than 600 "phishing" emails were sent to Mr. Azima and other individuals associated with him (and/or adverse to the government of RAK) in 2015 and 2016. Searches for those emails has identified a substantial number (more than 150), which have been analysed by a computer forensics expert, Mr. Tarbell, who provided an expert report for the trial and is formerly of the FBI. Mr Tarbell concludes that these emails were sent by the same hacker or group of hackers working together. Mr Azima seeks to rely on those emails, on Mr Tarbell's further report and the related parts of this witness statement, and on the data received from Mr Satter, in support of his case that RAKIA was responsible for the hacking of his data.
  - b. Second, there is a witness statement from Mr. Pourya Nayebi dated 17 August 2020. Mr Nayebi was one of the three individuals who agreed to purchase the Sheraton Metachi Hotel in Tblisi from RAKIA Georgia. Mr. Nayebi unambiguously states that Mr. Azima introduced him and the other buyers to RAKIA. Mr. Azima seeks to rely on this statement in support of his case that he was entitled to the payment he received from RAKIA for referring the buyers for the Hotel to RAKIA.
7. Mr. Azima also seeks to amend his grounds of appeal in view of this new evidence, and to rely on a short supplementary skeleton argument addressing those grounds.

8. Second, this new evidence also supports Mr Azima's application for a stay of the judgment debt and the interim payment on account of the costs of the proceedings below.
9. Finally, this witness statement responds to RAKIA's application issued on 19 August 2020 in which RAKIA applies for an order making permission to appeal (or continuation of the appeal, if permission is granted) conditional on Mr Azima paying the judgment debt and the interim payment on account of costs (**'RAKIA's Application'**). The new evidence provides a strong basis for dismissing that application, along with other reasons, addressed below.

### **III. The decision under appeal**

10. The factual background is summarised in the main judgment of Mr Lenon QC (**'Judgment'**) at §§13-57. As set out in the Judgment, the Claimant/Defendant to Counterclaim ("**RAKIA**") sued Mr Azima in misrepresentation and conspiracy, relying on a substantial quantity of Mr Azima's stolen data. RAKIA admits that the materials are stolen and the result of hacking, but claims itself to have obtained them innocently despite their explanations for how they came upon the hacked data being disbelieved by the trial Judge. In addition to resisting the merits, Mr Azima alleged that RAKIA was responsible for the hacking and sought the dismissal of the claims as an abuse of process or exclusion of the relevant evidence, and brought a Counterclaim for damages caused by the hacking which would serve as a set-off as to all of the claimed sums
11. The trial took place in January-February 2020 and the main judgment was delivered on 22 May 2020. The Deputy Judge upheld RAKIA's claims and found RAKIA's responsibility for the hacking unproven (Judgment, §381), and so also dismissed Mr Azima's counterclaim.
12. By an Appellant's Notice filed on 7 August 2020, Mr Azima seeks permission to appeal against the Judgment in each of these respects. He also seeks a stay of the judgment debt, which falls due on 28 August 2020.

### **IV. Evidence as to further 'phishing' emails**

#### **A. Summary**

13. As explained below, new evidence has come to light (through a tip off by Thomson Reuters) indicating that not only Mr. Azima but also other individuals associated with him and regarded by RAK as its enemies were targeted with malicious 'phishing' emails in a single campaign. The targets of this campaign include the individuals identified by the RAK government as its adversaries in the 'RAK Project Update' document of 26 March 2015 (**DPH8/1-17**), for their work on a campaign to publicise human rights abuses in RAK. The new evidence shows that the phishing campaign began at the same time as the Project Update was provided to RAKIA and the Ruler of RAK and continued until immediately before the publication of Mr. Azima's stolen data online.

## B. Background

14. On 8 April 2020, Mr. Satter (Cyber Security Correspondent for Thomson Reuters) (“**Mr. Satter**”) contacted Mr Azima’s US legal team (Laura Ferguson of the firm Miller & Chevalier) to explain that TR were working on a story<sup>1</sup> that touched upon Mr. Azima and the hacking of his emails.
15. Without any waiver of privilege, at my firm’s instruction, Mr. Tim Maltin of Maltin PR (a litigation support and public relations firm acting for Mr. Azima) communicated with Mr Satter on Mr. Azima’s behalf in order to obtain evidence and information for use in these proceedings. I also had some direct communications with Mr Satter. The evidence I give below is based on documentary materials provided to Mr Azima’s advisers and Mr. Maltin’s reports to me of his communications.
16. Between 27 April 2020 and 17 August 2020, Mr Azima’s advisers received a series of tables listing data about ‘phishing’ emails sent to Mr Azima and individuals associated with him (who would be considered adversaries by the government of RAK), indicating that they were the subjects of an extensive and highly targeted phishing campaign. Mr Satter indicated that, according to his firm’s investigation and to confidential sources, these emails were sent – and the campaign carried out by – a ‘hack for hire’ organisation.
17. Mr Satter indicated that he did not have the phishing emails themselves. However, the data he provided includes the timestamp when they were sent, the target’s details (i.e. the email address of the recipient) and the spoof sender details (i.e. the fictitious email address of the sender, which would appear on the face of the email to be the real sender). Mr Satter requested that, in return, Mr. Azima’s team provide the ‘native’ form emails that were received and retained so as to progress his investigation.
18. Further tables of data followed, the most recent of which was received in the week of 17 August 2020. Mr Satter informed Mr. Maltin that the information as to these phishing emails derives from a confidential source, whose identity he would not reveal. Mr Satter has also explained that the data he had obtained may be incomplete and that there may have been other phishing emails sent as part of the campaign.
19. Together, the information received from Mr. Satter strongly indicates that Mr Azima and his associates who were involved with RAK were sent more than 600 phishing emails by the same ‘hack for hire’ organisation between March 2015 and when Mr Azima’s hacked data was published on BitTorrent websites in early August 2016. Copies of the tables received are attached at **DPH8/19-76**. Without any waiver of privilege, an example of an email providing such a table is at **DPH8/18**. A master list

---

<sup>1</sup> On 9 June 2020, TR and Citizen Lab (a research group focusing on information and communication technologies, human rights, and global security) released stories on ‘hack for hire’. These stories (TR: (**DPH8/108-119**) and Citizen Lab: (**DPH8/77-107**)) indicated that TR and Citizen Lab had worked closely on their investigation into this murky and clandestine world. TR identified a company, Bell Trox Info Tech Services (“**Bell Trox**”) as involved in a series of hacks between 2015 to date (**DPH8/108-119**). Citizen Lab referred to a ‘hack for hire’ “group” which it described as “Dark Basin”, and which it stated was connected to Bell Trox. These stories do not report on the hacking of Mr Azima. Mr Azima does not seek (and does not need) to prove that Bell Trox was the specific legal entity responsible for the hacking attack on him. He does however consider that the phishing campaign was likely carried out by a ‘hack for hire’ individual or group which he infers, for the reasons I have set out in this statement and the points made by Mr. Azima at Trial, was acting on RAKIA’s instructions.

compiling this information into a single spreadsheet (prepared by Mr. Azima's advisers) is attached at **DPH8/166-177**.

20. As noted in Mr. Tarbell's report dated 24 August 2020, phishing emails attempt to evoke an action from the recipient, most commonly by tricking the recipient into clicking a link or opening an attachment to the phishing email. Cyber criminals mislead the email recipients by attempting to mimic well-founded organizations or use personal details within the fake email to make the recipient feel the sender is known and / or genuine. Once the phishing email recipient's confidence has been gained, the recipient may be led into opening an attachment to the email that includes malware, or a link in the email may direct the recipient to malicious servers or to a fabricated login screen used to steal usernames and passwords.
21. The data provided to Mr Azima's team indicated that, in addition to Mr Azima, a range of individuals were targeted with phishing emails. As explained further below, each of these individuals was regarded by RAK as aligned with Mr. Azima and/or adverse to RAK. They include: Dr. Khater Massaad (CEO of the RAK Investment Authority), Mr. Christopher Cooper (PR consultant, who is named in a RAK internal report, the 'RAK Project Update' as part of a team managed by Mr. Azima seeking to publicise alleged human rights abuses in RAK), Mr. Kirby Behre (US counsel to Mr. Azima and Dr. Massaad, who is named as part of the team seeking to publicise human rights abuses), Mr. Gary Bernstein (who conducted investigations into human rights abuses in RAK and provided reports to Mr. Azima and his team), Ms. Afsaneh Azadeh (business associate of Mr. Azima and General Manager of HeavyLift, one of Mr. Azima's companies), Ms. Cynthia Beudjekian (PA to Dr Massaad), and Mr. Ray Adams (CFO for Mr. Azima and HeavyLift).
22. Schedule 1 to this witness statement sets out the details of these individuals with associations with Mr. Azima to whom (according to the data received) phishing emails were sent.
23. Mr. Azima's team used the spreadsheets of email data provided to locate corresponding native emails received by Mr. Azima and these individuals. This yielded 104 native emails received in thirteen email accounts held by the individuals referred to above.
24. These emails were obtained by Mr. Azima's advisers between May – August 2020. Not all of the individuals are under Mr Azima's control and so (while efforts were made to obtain the evidence as quickly as possible) the process took some time.
25. In my view, it is significant that these individuals discovered a substantial number of the emails which had been referred to in the data provided by Mr Satter of Thomson Reuters. This suggests that the data provided is reliable (it being confirmed that a substantial number of the emails in the tables had been received). Other emails in the tables were not found perhaps because they were deleted near the time received or were caught by the recipient's spam filter and so deleted automatically over time.



26. In addition, searches were made by Mr. Azima and these other individuals for other phishing emails. This was because, as noted, Mr Satter had advised that the data he provided may not provide a complete set of the phishing emails. These searches were made by searching for technical information identified by TR as a phishing technique.<sup>2</sup> This yielded further emails. In total, some 175 emails were identified as potential phishing emails to be investigated further.

C. Mr. Tarbell's Report Dated 24 August 2020

27. These 175 emails were then provided to Mr. Tarbell, the forensic IT expert who provided a report on Mr Azima's behalf at trial, to analyse to determine the following:

*(1) In your view, are these emails (or any of them), 'spoof'/phishing emails. If so, please confirm which emails you consider are spoof / phishing emails and why.*

*(2) By reference to the content, style, format, headers and metadata (and any other characteristics) of the emails, are there any commonalities between the emails (or a number of them) which might point to them being sent by the same malicious party. If so, please identify the group of emails and the features which make them related.*

28. Mr. Tarbell's report is exhibited at **DPH8/123-155**. As Mr. Tarbell explains in his report, out of the 175 emails I provided to him, he has identified 153 unique, native emails which he has then analysed as part of his report.
29. The Court is respectfully invited to read Mr. Tarbell's report, but the key findings are as follows.
30. The 153 emails span 13 different email accounts belonging to Mr Azima, Mr Cooper, Mr Behre, Dr Massaad, Mr Adams, Ms Azadeh and Ms Beudjekian. Mr Tarbell found that all of the emails in the set were phishing emails. He also identified several common technical characteristics used by cyber criminals in phishing across the set of emails. He noted that the vast majority:
- a. used the same service – MESVR – to conceal the real sender or the nature of links contained in the email from the recipient (97% of emails in the set);
  - b. used a specific service that provides the sender with a notification that the recipient had opened the email and other information as to the recipient, including their IP address, browser type, location and the time for which the email remained open (93% of emails, all of which also used MESVR);

---

<sup>2</sup> TR advised that a specific service – known as MESVR – was used by the hack for hire organisation as a 'wrapper' for phishing emails, concealing the real identity of the sender or links contained in the email. Searches were conducted for emails indicating that MESVR had been used.

- c. contained one or more unusual and distinctive sound and image files, that were likely connected to a specific account of the notification service mentioned in (b) above (96% of emails);
  - d. contained the same falsified content in the email headers, that appeared to have been included in an attempt to bypass the recipient's spam filters (90% of emails);
  - e. had been sent using a 'fake mailer', which counterfeits the name and address of the sender and adds other false information to an email header (67% of emails); and
  - f. were sent within the same 8 hour time window (5:40am UTC and 1:39pm UTC) (89%) on different days (but not on Sundays), suggesting that the hacker (or group of hackers working together) was located in a single timezone and had particular working habits.
31. The results of Mr. Tarbell's analysis are set out in more detail in his report and the spreadsheets attached to it.
32. Importantly, Mr Tarbell concludes based on the characteristics of these phishing emails that they were sent by the same hacker (or group of hackers working together).

D. Connections between these emails and Mr Azima's allegation of hacking by RAKIA

33. The identity of the recipients and the dates on which these emails were sent points strongly towards RAKIA's responsibility for this hacking campaign.
34. **RAK Project Update** A focus of the hacking issue at trial was on a document dated 26 March 2015, the 'RAK Project Update'. A copy is attached at **DPH8/1-17**. The unredacted parts of the document are fairly short. It is described in the Judgment (§32):

"In March 2015 Mr Page provided the Ruler with a report entitled RAK Project Update ("the Project Update") which was mainly concerned with Dr Massaad's activities but which also described how Mr Azima was managing a team of advisers in the US, hired by Dr Massaad, who were planning to spread allegations about human rights issues in RAK; their campaign had not yet been made public. Mr Page's agents who compiled the report said that they would be able to gather intelligence on the campaign team in order to monitor their progress and "attempt to contain or ruin their plans". "

35. The Project Update is described in more detail at §§260-278. The Judge found that RAKIA's witnesses deliberately minimised the Project Update in their written evidence. The author of the Project Update, Mr Page, had in fact concealed his role completely,



falsely stating that he only provided reports orally and that he had not heard of Mr Azima until 2016. These matters form part of Mr Azima's appeal (in particular grounds 1, 3 and 4).

36. The Judgment quotes a passage of the Project Update which identifies key figures in the US team being managed by Mr Azima (§267):

"In the US, KM's hired a team of advisors managed by Farhad Azima (FA) in order to spread allegations against our client. The main allegations against the client are on human rights issues and in particular the allegation that RAK uses a dedicated facility in RAK where it imprisons and torture political opponents. FA, who might also be responsible for paying the US team, handles all KM's activities in the US. KM's lawyer in the US, Kirby D. Behre, hired a consultant, who is a former WSJ reporter, named Christopher Cooper, who due to his good contacts. Cooper approached a British reporter named Simon Goodly of The Guardian and briefed him on the RAK torture allegations, in order to raise public opinion against RAK and to harness international civil rights organizations to the subject."

37. The Project Update thus identifies Dr Massaad, Mr Azima, Mr Cooper and Mr Behre as individuals engaged in the campaign concerning allegations of human rights abuses.

38. I respectfully suggest that it is striking that phishing emails (that Mr Tarbell concludes were sent by a single hacker or group of hackers working together) were sent to each of these individuals. This strongly supports Mr Azima's case at trial that the Project Update led the Ruler of RAK to order surveillance of Mr Azima, at least part of which was carried out through hacking. The Judge found as follows as to the Ruler's motivation following the Project Update (at §290):

"It is more likely that the Ruler's hostility towards Mr Azima stemmed from his perception, originating in the Project Update, that Mr Azima was an associate of Dr Massaad who was threatening to cause trouble for him."

39. **Timing of phishing emails** The dates on which the phishing emails were sent also supports the view that RAKIA was responsible. As set out in the spreadsheet attached to Mr Tarbell's report (see first tab: "153 Emails Chronologically"):

- a. Multiple phishing emails were sent to Mr Behre on 26 March 2015, the same date as the RAK Project Update, and for the following week.
- b. Mr Azima was then sent multiple phishing emails between 7 and 10 April 2015. These followed an instruction given by the Ruler to his advisers to "target" Mr Azima on around 4 April 2015. The Judge dealt with this "targeting" email (and other similar emails) at Judgment, §§279-292. As noted above, the Judge found that the Ruler's instructions to his advisers were motivated by his hostility for Mr Azima, stemming from the Project Update.

- c. A large number of phishing emails were also sent to Mr Cooper in April and May 2015, shortly after the Project Update and following the "targeting" emails.
  - d. Ms Azadeh, a HeavyLift employee, was introduced to RAKIA by Mr Azima in mid-June 2015, to discuss HeavyLift's claim for compensation (see Judgment, §129.4). This was followed by a more detailed letter sent by Ms Azadeh to RAKIA on 6 July 2015 (written by Mr Adams, another business associate of Mr Azima). Ms Azadeh received phishing emails beginning on 14 August 2015, and many times thereafter. Phishing emails were also sent to Mr. Adams from September 2015.
40. **Conclusion** In my respectful view, the only cogent explanation for these phishing emails being sent to all these individuals at these times was that they were sent on behalf of RAKIA. It is highly improbable that any party other than the government of RAK and its advisers would send phishing emails to Mr Cooper, Mr Behre, Dr Massaad, et al., at this time.

E. The phishing campaign revealed by TR's data of emails sent

- 41. As explained above, the data provided by Mr Satter of Thomson Reuters indicates that more than 600 phishing emails were sent to Mr. Azima and associated individuals between March 2015 and August 2016.
- 42. In my respectful view, that information should be regarded as credible given that a substantial number of emails corresponding to the data provided were found in the inboxes of Mr. Azima and his associates. The fact that other emails are not available is explicable and to be expected: these emails were sent 4-5 years ago and many would have been either deleted by the recipients, or were caught by the recipient's spam filter and so deleted automatically.
- 43. Examination of the data provides compelling confirmation that Mr. Azima and the other individuals associated with him (and named in the Project Update) were the target of a single campaign. The data shared by Mr Satter as part of his investigation for Thomson Reuters is set out in the spreadsheet at **DPH8/156-177**, which orders the phishing emails by date (tab 1) and by sender (tab 2).
- 44. Even a passing examination of this master list confirms that the phishing emails were sent in a single campaign. To take a handful of examples only:
  - a. In tab 2 (ordered by sender), as shown in rows 2 and 3, phishing mails were sent to Dr Massaad and Mr Cooper on 5 May 2015 within 4 minutes of each other, from the same spoof sender. This indicates that the hacker simply sent the same spoof email twice, to different recipients as part of the same phishing campaign.
  - b. The same pattern – of an email being sent from the same spoof sender to Dr Massaad and Mr Cooper within a short period on the same day – can be observed over and over again at rows 4-18, 33-36, 60-61, 176-177 and many

others. These emails were sent in April and May 2015, shortly after the Project Update.

- c. Similarly, at rows 38-41, emails from the same spoof sender were sent to four different recipients (Mr Azima, Dr Massaad, Ms Azadeh and Mr Behre) within an hour on the same day.
  - d. All of Mr Azima, Dr Massaad, Mr Adams, Ms Azadeh, Mr Berntsen and Mr Behre were sent an email from the same spoof sender within a 3 hour period on the same day (rows 212-217) and within a 2 hour period on another day (rows 158-163).
45. Taken with Mr Tarbell's analysis of the native emails that have been found, I submit that the data shared by TR as part of their ongoing investigation into hacking makes it plain that these phishing emails were sent by a single hacker or group of hackers working together in a coordinated campaign.

F. Admission of this evidence in the appeal

46. I respectfully submit that the evidence based on the analysis of emails described above satisfies the test for the admission of fresh evidence in an appeal (as explained in *Ladd v Marshall* [1954] 1 WLR 1489).
47. I would note the following matters as to the question whether the evidence could have been available with reasonable diligence at the time of the trial:
- a. The prompt for this further investigative work to be done originated from tables of data received from Mr Satter between April 2020 and late August 2020. Finding the corresponding native emails for these then required the cooperation of third parties.
  - b. The data provided strongly indicated that the hacking of Mr Azima was part of a much wider attempted hacking of those associated with Mr. Azima and RAK business. This was a new lead in the case.
  - c. The Court of Appeal has recognised that the "reasonable diligence" requirement is applied more flexibly (or not applied at all) in instances of fraud: see *Meek v Fleming* [1961] 2 QB 366, 381. It would be appropriate to take such an approach here. It is self-evidently particularly difficult to investigate serious and covert wrongdoing such as email hacking. These difficulties were particularly acute in this case as RAKIA had concealed Mr Page's authorship of the Project Update (see Judgment, §§265, 271). This was also significant given that Mr Page has been linked to hacking in other cases (Judgment, §§368-369).
48. I respectfully suggest that the other requirements of the *Ladd v Marshall* test are also met:

- a. The evidence would have an important influence on the result of the case. The Judge found a range of evidence supporting Mr Azima's case that Mr Page had procured the hacking on RAKIA's behalf (Judgment, §377). It is in the nature of a circumstantial case that an additional piece of evidence (even circumstantial evidence) may be decisive, when taken with the other evidence. Taken with the other evidence that the Judge recognised supported Mr Azima's case, this evidence would clearly have an important influence; indeed, while the evidence need not be decisive, in this instance it should be.
  - b. The evidence is not merely a marginal addition to the compelling case that RAKIA was the instigator of the hacking. It is evidence which is difficult to reconcile with any other conclusion.
  - c. The evidence is also 'apparently credible': it is based on documentary evidence (the 'phishing' emails) to which Mr. Azima was alerted by a reputable third party (TR), read with the analysis of a qualified expert (whose evidence was not challenged at trial by RAKIA). The credibility of this information has been confirmed by the fact that more than 100 emails were found, matching that information. The forensic power of those emails then emerges from assessing the recipients and the timing in light of the individuals who featured in the RAK Project Update, a document which the Judge described as important and on which he placed substantial weight (Judgment, §§272, 377.1).
49. In addition to the appeal, this evidence is also clearly relevant and material to the questions of the stay sought by Mr Azima, and RAKIA's Application. I address these points further below.

**V. Witness Statement of Pourya Nayebi**

50. At **DPH8/120-122**, I enclose the witness statement of Mr. Pourya Nayebi dated 17 August 2020.
- A. The Hotel transaction
51. By way of background, Mr. Nayebi is one of three businessmen who sought to purchase the Sheraton Metachi Hotel ("**the Hotel**") in Georgia in 2011 from RAKIA Georgia ("**the Hotel Transaction**").
52. One of the issues at trial was whether or not Mr. Azima introduced Mr. Nayebi and his partners to the Hotel Transaction. RAKIA claimed that Mr. Azima had falsely claimed to have made that introduction as a basis for claiming payment of a commission (of US\$1,562,5000) from RAKIA. RAKIA's case was that Mr. Azima created a sham referral agreement claiming an entitlement to this payment for the introduction and (since he had no legitimate entitlement to payment) he then bribed Dr. Massaad, the then CEO of RAKIA, to secure the payment of the commission. The Judge summarised the parties' cases at §23:

"Mr Azima received two payments of \$400,000 and \$1,162,500 on 25 October 2011 and 18 January 2012 respectively and, on the day that he received the latter of those payments, Mr Azima made a payment of \$500,000 to Dr Massaad. Mr Azima's case is that he was entitled to both payments under a referral agreement with RAKIA ("the Referral Agreement") as commission for introducing to RAKIA three Iranians who were potential buyers of the Hotel ("the Potential Buyers") and that the payment to Dr Massaad was in return for a share in an aircraft owned by Dr Massaad. This version of events is disputed by RAKIA which contends that the Referral Agreement is a sham, that Mr Azima did not introduce the Potential Buyers, that the two payments which he received were misappropriations and that his payment to Dr Massaad was a bribe."

53. It was Mr. Azima's case at trial that RAKIA's allegations were flatly contradicted by the contemporaneous documents and were misconceived because they rested on a flawed premise; namely that Mr. Azima had no entitlement to any referral fee because he had not introduced the buyers to the transaction.
54. On the issue as to whether Mr. Azima had introduced the buyers to RAKIA, the Judge's analysis of evidence is set out in §§168-173 of the Judgment, and his conclusions are at §§174-177. The Judge found that much of the evidence supported Mr Azima's case that he had made the introduction and that RAKIA's case to the contrary was not supported by contemporaneous documents or witnesses who were prepared to be cross-examined (Judgment, §§174-175 – emphasis added):

"Discerning the role of Mr Azima in relation to the intended Hotel transaction is not straightforward. **There were no independent witnesses**. None of RAKIA's witnesses was in a position to give first-hand evidence of the relevant events apart from the Ruler, who did not attend the trial and whose evidence therefore carries limited weight. RAKIA did not produce any contemporaneous documents relating to the planned sale of the Hotel and the documents relied on by Mr Azima were inconclusive. The photographs and the emails showed that that Mr Azima certainly had meetings with the Potential Buyers and was actively involved in facilitating the possible purchase. But they fall short of establishing that Mr Azima was instrumental in actually introducing the Potential Buyers to the transaction.

\*\*\*  
"Contrary to RAKIA's case, the short interval between the date of the alleged introduction and the signing of the MoU does not, in my judgment, preclude the possibility that Mr Azima's [sic] effected the introduction.

55. The Judge was ultimately swayed in RAKIA's favour by a memorandum prepared by Mr Adams, a business associate of Mr Azima, in March 2016 (more than 4 years after the transaction): Judgment, §176. Mr Azima's case was that the memorandum was mistaken in this respect and was prepared for a purpose in which the introduction of the buyers to RAKIA was not material.

56. A fair reading of the Judge's reasons would suggest that – in the absence of independent witness evidence or conclusive contemporaneous documents – the point was in the balance and that Mr Adams' memorandum was the best evidence available.
57. However, it is now clear that there is independent witness evidence – unavailable at trial – that shows this conclusion to be wrong. Mr Nayebi explains (at §9):

“...our introduction to RAKIA was through Mr. Azima. He introduced me, Mr. Hosseinpour and Mr. Farsoodeh to the prospective transaction of purchasing the Hotel. I believed him to be very important to that transaction he was heavily involved in negotiations and liaising between all the parties. Without Mr Azima I would not have known that the Hotel was for sale and I was not introduced to the transaction by anyone else”.

58. Mr Nayebi explains his reasons for providing this statement at this stage, at §10:

“In the past several years, I have had very little contact with Mr. Azima having had a fall out over the Hotel transaction. However, upon seeing the Judgment handed down in this case, reviewing the sections of that Judgment which deal with the Hotel transaction and also reading in the press and media that Mr. Azima intends to appeal the Judgment, I considered that I owed it to Mr. Azima to set the record straight to avoid a miscarriage of justice taking place. This is especially so given the findings which have been made against Mr Azima based on wrong and false information, including the finding that he did not introduce me, Mr. Hosseinpour and Mr Farsoodeh to the transaction, which I can confirm is entirely incorrect.”

**B. Consequences of Mr Nayebi's evidence**

59. The Judge relied on his finding that Mr Azima had not introduced the buyers to RAKIA in two critical respects.
60. First, he relied on that finding to conclude that a referral agreement prepared by Mr Adams was a 'sham': see Judgment, §181.3.
61. Second, he relied on this finding in order to conclude that Mr Azima's payment of \$500,000 to Dr Massaad was a bribe, since (absent any introduction) Mr Azima would not have been entitled to any commission (Judgment, §186 – emphasis added):

**“Conclusion**

RAKIA's case that the payment of the \$500,000 was a bribe paid to Dr Massaad rests essentially on the inference to be drawn from the fact that the payment was made on the date Mr Azima received a fee authorised by Dr Massaad to which he had no entitlement and the absence of any convincing alternative explanation for the payment.”

62. If, as Mr Nayebi's evidence states, Mr Azima did introduce the buyers to RAKIA, then these two conclusions are unsound, as would be the Judge's finding against Mr. Azima in conspiracy.



C. Admission of this evidence

63. **Appeal** I respectfully submit that Mr Nayebis' witness statement Nayebi satisfies the test for the admission of fresh evidence in an appeal.
64. As to the requirement that the evidence could not with reasonable diligence have been adduced at the trial:
- a. Until recently, Mr. Nayebi was (as he confirms) unwilling to be a witness. Mr. Azima and Mr. Nayebi had an adversarial relationship since 2015. Mr. Azima had sued Mr. Nayebi in the UAE relating to a business transaction. In addition, Mr. Nayebi was on a list of individuals subject to sanctions by the US government. Mr. Azima understands Mr. Nayebi to have held Mr. Azima to be responsible for those sanctions being imposed. Mr. Nayebi and Mr. Azima had therefore fallen out and were not in contact prior to the trial. It had been the understanding of Mr Azima's team that Mr. Nayebi was cooperating with RAKIA in other litigation.
  - b. Mr Nayebi is also resident abroad (in Iran) – accordingly it was not open to Mr. Azima to summon Mr. Nayebi to give evidence.
  - c. However, following the judgment being published and associated media coverage, Mr. Nayebi then contacted Mr. Azima and, through solicitors, provided this witness statement on 17 August 2020. Mr. Azima understands Mr. Nayebi to have felt an attack of conscience and to have decided to assist him in correcting what he considered to be a miscarriage of justice.
65. The evidence is also 'apparently credible': it emanates from an independent third party who was adverse to Mr. Azima and who was directly involved in the events at issue. The evidence would also have an important influence on the case: as explained above, the Judge's finding as to the introduction was a material basis for his conclusion on the allegations of both a 'sham' agreement and a bribe.

VI. Stay / RAKIA's Application

66. Mr. Azima also relies on this new evidence in support of his application for a stay of the judgment below, and in opposition to RAKIA's application of 19 August 2020.

A. Stay

67. For the reasons set out above, I submit that the new evidence clearly fortifies Mr. Azima's case that RAKIA was responsible for the hacking of his emails and creates a compelling inference to that effect. If RAKIA was responsible for the hacking, there would be good grounds for its claims to be struck out as an abuse of process (as the Judge acknowledged: Judgment, §384), and Mr. Azima's counterclaim could also

proceed. In those circumstances, rather than Mr. Azima being liable to RAKIA, RAKIA would be liable to Mr. Azima for very significant losses.

68. The new evidence from Mr Nayebi clearly places the Judge's finding in conspiracy in doubt and thus the award of damage made on that basis.
69. In the premises, it would be unjust for Mr. Azima to be required to pay the judgment debt (and the interim payment on account of the costs of the proceedings below) until his appeal has been determined, particularly where the payment would be made to a party whom the evidence indicates is culpable for serious wrongdoing.
70. I would also note that RAKIA's response to Mr. Azima's application for a stay does not demur at all from the point made in the application that any judgment debt paid to RAKIA would pass out of its hands and beyond its control. Moreover, while RAKIA contends that there is 'no evidence' of its unreliability, Mr Azima's application for a stay set out in detail the facts showing that, when ordered by the Court to provide a pleading explaining how it came to possess the hacked material, it provided a false account. This is damning evidence on its unreliability.

**B. RAKIA's Application**

71. RAKIA's Application was made without any attempt in advance to engage with Mr Azima's solicitors or any explanation for failing to do so. Had RAKIA done so, the scope of matters in dispute would have been narrowed, as Mr Azima is willing to provide security for the costs of his appeal in the event permission is granted, in the amount sought (but would seek to provide this security at the same time as the appeal skeleton is lodged, in the event permission is granted).
72. RAKIA's Application otherwise seeks to make payment of the judgment debt a condition of permission to appeal, or the appeal itself progressing. On its face, this is an attempt to stifle an appeal that would explore its wrongdoing, and which the Judge clearly erred in finding was unproven. It is striking that this application has been made before the judgment debt has become due or the Court has even had the opportunity to consider the merits of the appeal. If this Court considers that there is sufficient merit in the appeal for permission to appeal to be granted, it should be allowed to proceed regardless of whether the judgment debt has been satisfied.
73. Contrary to RAKIA's reasons for its Application (§6) Mr Azima does not accept that he was in breach of orders and it is notable that RAKIA does not give any examples. Both Mr Azima and RAKIA on occasion sought additional time to comply with deadlines (with Mr Azima agreeing to RAKIA's requests). It is notable also that on those occasions that Mr Azima was ordered to pay RAKIA's costs (and costs were on occasion also ordered against RAKIA), he did so when required.

74. The Court's assessment of an application for a condition to be impose on appeal should be considered in light of the justice of the case and all the circumstances. The new evidence set out above shows the judgment below to have reached the wrong conclusion and so provides a compelling basis for refusing to impose such a condition.

**Statement of Truth**

I believe that the facts stated in this witness statement are true. I understand that proceedings for contempt of court may be brought against anyone who makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth.

**Signed:** *Dominic Holden*  
**Name:** **Dominic Holden**  
**Position:** **Partner, Burlingtons Legal LLP**  
**Dated:** **24 August 2020**

**Schedule 1**

<b>Name</b>	<b>Email address</b>	<b>Connection to Mr. Azima</b>
Farhad Azima	hh@fathers.church farhad@farhadazima.com farhad.azima@algkc.com fa@fa1.us fazima@gmail.com	
Khater Massaad	cardinal@fathers.church khatermassaad@starinvests.com Kmoffice@starindustrialholding.com accounting@starindustrialholding.com	CEO of RAKIA until 2012. Mr Azima was described in the 'RAK Project Update' document of 26 March 2015 as managing a US team for Dr Massaad, with a view to publicising allegations of human rights abuses in RAK.
Christopher Cooper	ccooper@potomacsquaregroup.com Cooperjournal@gmail.com	PR consultant. Named in the RAK Project Update document as part of the US team seeking to publicise allegations of human rights abuses in RAK.
Kirby Behre	kirbybehre@gmail.com	Named in the RAK Project Update as part of the US team working to publicise allegations of human rights abuses. Lawyer at Miller & Chevalier (Mr. Azima's and Dr. Massaad's US attorneys in 2015 / 16).
Gary Bernsten	vicar@fathers.church	Former Senior CIA officer and former shareholder and

		CEO of Denx LLC. Mr. Berntsen worked with Mr. Azima in 2015 on efforts to publicise allegations of expose human rights abuses in RAK.
Afsaneh Azadeh	afsaneh@algkc.com afsanehazadeh@gmail.com afsanehazadeh@yahoo.com Sarabrightman66@yahoo.com	Senior employee of Mr. Azima's companies. Presented information to RAKIA in support of a claim for compensation by HeavyLift (one of Mr Azima's companies)
Cynthia Beudjekian	Cynthia.b@starindustrialholding.com cynthia.b@starinvests.com	Dr. Massaad's secretary.
Bernard Gilbert	b.g.massaad@starindustrialholding.com	Dr. Massaad's son
Ray Adams	Ray.Adams@algkc.com loyd.ray.adams@icloud.com cfo@alg-marine.com Ray@jffintl.com jff@jffintl.com ray.adams@tasman.com	Long-time associate of Mr. Azima and chief financial officer of several of Mr. Azima's companies. Presented information to RAKIA in support of HeavyLift's claim for compensation.

Filed on behalf of the Proposed Appellant  
Eighth witness statement of Dominic Holden  
Exhibit: DPH8  
Date: 24 August 2020

**Claim No.: HC-2016-002798**

**IN THE HIGH COURT OF JUSTICE**  
**BUSINESS AND PROPERTY COURTS OF**  
**ENGLAND AND WALES**  
**BUSINESS LIST**

---

**FARHAD AZIMA**

**Proposed Appellant /**  
**Defendant and Counterclaimant**

**-and-**

**RAS AL KHAIMAH**  
**INVESTMENT AUTHORITY**  
**Proposed Respondent /**  
**Claimant and**  
**Defendant to Counterclaim**

---

**Burlingtons Legal LLP**

5 Stratford Place  
London W1C 1AX  
Ref: DPH/AZI.3/2  
Solicitors for the Proposed Appellant



